

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

) 4:21 MJ 349 DDN

INFORMATION ASSOCIATED WITH OMEGLE

ACCOUNT WITH COOKIE ID JSDY9Z4U THAT IS

STORED AT PREMISES CONTROLLED BY

OMEGLE.COM LLC

) FILED UNDER SEAL

) SIGNED AND SUBMITTED TO THE COURT FOR

) FILING BY RELIABLE ELECTRONIC MEANS

)

APPLICATION FOR A SEARCH WARRANT

I, Jeremy L. Weadon, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the _____ District of Washington, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- xx evidence of a crime;
- xx contraband, fruits of crime, or other items illegally possessed;
- xx property designed for use, intended for use, or used in committing a crime;
- xx a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

Title Section

Title 18, United States Code, Sections 2251(a) (sexual exploitation of children), 2252A (certain activities relating to material constituting or containing child pornography), 2422 (coercion and enticement of a minor) and/or 1470 (transfer of obscene material to a minor)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.



Applicant's signature

Jeremy L. Weadon, TFO, FBI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date 12/16/2021

/s/ David D. Noce

Judge's signature

City and State: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge

Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH) No. 4:21 MJ 349 DDN
OMEGLE ACCOUNT WITH COOKIE)
ID JSDY9Z4U THAT IS STORED AT) **FILED UNDER SEAL**
PREMISES CONTROLLED BY)
OMEGLE.COM LLC) SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jeremy L. Weadon, Task Force Officer, Federal Bureau of Investigation (FBI), having been duly sworn, hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Omegle.com LLC (hereinafter the Provider), a social media and electronic communications service/remote computing service provider headquartered at 906 West 2nd Ave, STE 100, Spokane, WA 99201. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require the Provider to disclose to the United States and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications as further described in Attachment B.

2. I am a Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”), assigned to the FBI office in St. Louis, Missouri, and assigned to investigate Internet Crimes Against Children. I have been a TFO with the FBI since March 2019. As part of my

duties, I investigate violations of federal law, including the online exploitation of children, particularly in relation to violations of Title 18, United States Code, Sections 2251, 2252, and 2252A which criminalize, among other things, the production, advertisement, possession, receipt, distribution, and transportation of child pornography.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of children), 2252A (certain activities relating to material constituting or containing child pornography), 2422 (coercion and enticement of a minor) and/or 1470 (transfer of obscene material to a minor) have been committed by Gregory Ortlip. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

LOCATION TO BE SEARCHED

5. This warrant applies to information associated with Omegle account associated with Gregory Ortlip, Cookie ID JSDY9Z4U that is stored at premises owned, maintained, controlled, or operated by Omegle.com LLC, a company headquartered at 906 West 2nd Ave, STE 100, Spokane, WA 99201.

6. The Omegle account associated with Gregory Ortlip is fully described in Attachment “A”. A Preservation Request was submitted on August 13, 2021, by Missouri State Highway Patrol Trooper Jack Frost.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

INFORMATION REGARDING OMEGLE

8. Omegle is a free anonymous online chat website that allows users to talk with strangers. There are two main modes, “text” for plain text-based chats and “video” which allows the use of webcams. The service randomly pairs users in one-on-one chat or video sessions where they chat anonymously using the names “You” and “Stranger.” The video chat also has a built-in text window. The site now also provides a mobile application that lets users chat with strangers from mobile devices.

9. Before being matched with a stranger to speak with, users have the option to input “interest” tags. Adding interest tags lets users be paired with a stranger who has something in common with the user. A user can input as many interest tags as he or she would like, and if no available match is found, the user is paired with a completely random stranger instead.

10. Omegle also has a “Dorm Chat” mode, which requires users to provide an email address ending in “.edu” to verify that they are associated with a college or university. Once users input an “.edu” email address, they receive an automated email from Omegle to confirm

their email address. Dorm Chat allows users to chat with other users that have an email address ending in “.edu” on Omegle.

11. In “Spy Mode,” Omegle users can pose questions to other users in a chat. Users have two options: to be the “spy” and ask a question of two strangers or to discuss a question with another stranger. As the spy, the user inputs any question for the two strangers to answer or discuss and is able to view the discussion as a third party, albeit without being able to contribute further to the conversation. The spy can quit at any time without ending the chat for the two other strangers. If a user chooses to discuss a question instead, as in normal text mode, the user is paired with another stranger and can discuss the question the spy has asked up until the point the other stranger decides to disconnect and/or move on to another question.

12. At the end of a “text” chat session, the user is given the option to save the text contents of chats (the “log”). If a user decides to save the log, Omegle gives the chat a log ID number and a URL. The user will need the URL to access a saved Omegle log. The user also has the option to post the log to social media websites like Facebook, Tumblr, Twitter, or Reddit. Once a user decides to save the log, Omegle will indefinitely retain any saved chat logs.

13. Omegle has both unmonitored and monitored video chat capability. Omegle implemented a “moderated” video chat to monitor misbehavior and protect people under the age of 18 from potentially harmful content, including nudity or sexual content. Omegle also has an “unmoderated” video chat that is not monitored for sexual content. Upon clicking on the option for the “unmoderated” section, Omegle warns users that they may be more likely to encounter sexual behavior in the “unmoderated” section. Omegle also added a warning to the homepage, stating “Predators have been known to use Omegle, so please be careful.”

14. Omegle does not have usernames, accounts, or registration. It collects IP addresses and also uses a cookie for identification. Omegle's ID cookie is a random value stored on users' computers, and it remains constant unless the user deletes it. To find a user's ID cookie on their computer, you can visit: <http://omegle.com/id>.

DEFINITIONS

15. The following non exhaustive list of definitions applies to this Affidavit and the Attachments to this Affidavit:

a. "Child Pornography" means any "visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8)(A).

b. "Visual depiction" includes "undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion to a visual image that has been transmitted by any means, whether or not stored in permanent form." 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated—(a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or

masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. 18 U.S.C. § 2256(2).

d. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” 18 U.S.C. § 1030(e)(1).

e. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. “Internet Service Providers,” or “ISPs,” are commercial organizations that provide individuals and businesses with access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet, including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name, such as a username or screen name, an e-mail address, and an e-mail mailbox. Typically, the subscriber creates a password for

the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

g. “Uniform Resource Locator” or “Universal Resource Locator” or “URL” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname—a hierarchical description that specifies the location of a file in that computer.

h. “Computer server,” or “server,” is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. The web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as “https://www.justice.gov/” into their web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so that the computer hosting the web site may be located, and the DNS server provides this function.

- i. “Hyperlink” refers to an item on a website that, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- j. “Internet Protocol address,” or “IP address,” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses can also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- k. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-Up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).
- o. “Contents,” as used with respect to any wire, oral, or electronic communication, includes “any information, concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).
- p. “Remote Computing Service” means “the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

q. “Electronic Communication Service” means “any service which provides to users thereof the ability to send or receive wire or electronic communications.”

18 U.S.C. § 2510(15).

r. “Electronic Storage” means “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17). Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage constitutes “electronic storage.”

s. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings, drawings, and paintings), photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies); mechanical form (including phonograph records, printing, and typing); or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers,

Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

**BACKGROUND REGARDING DIGITAL MATERIAL AND
CHILD EXPLOITATION**

16. Based on my training, my experience, and my discussions with other law enforcement agents, I know the following:

- a. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.
- b. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.
- c. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

d. Collectors, solicitors and distributors of child pornography also use online resources to obtain child pornography, including services offered by Internet Portals such as Google, Yahoo!, Facebook, and Omegle, among others. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

e. Collectors, solicitors and distributors of child pornography also target children through Internet-accessible mobile devices, social media applications, and chatrooms for sexual exploitation by "grooming" them to be receptive to sexual exploitation. Grooming is the method by which a pedophile may gain the trust of the child by psychological manipulation. These methods may include but are not limited to the use of gifts, trips, or other incentives for the purpose of sexually abusing the child. Pedophiles may also convince the child that s/he is a participant in a consensual romantic relationship in an attempt to normalize the sending of sexually explicit material. The offender may also use coercion and blackmail to force the child to send additional explicit material. These social media applications and chatrooms allow pedophiles access to a large number of potential victims and they will often use the same platform to victimize multiple children.

f. Omegle is among the social media platforms used by adults as an online resource to "meet" and groom children and ultimately produce, collect, and trade child pornography. Omegle's founder, Leif K-Brooks, has lamented the "x-rated"

way some users utilize Omegle, calling it “annoying.” To combat sexual material on the website, Omegle implemented “monitored” video chat. Omegle also added a warning to its users, “Predators have been known to use Omegle, so please be careful.”

DETAILS OF THE INVESTIGATION

17. On Friday, August 13, 2021, Detective Matt Hedden, Kentucky Office of the Attorney General, contacted the Missouri State Highway Patrol to ask for assistance with an ongoing criminal investigation. Detective Hedden initially talked to Trooper Jack Frost. Trooper Frost later referred the investigation to other Troopers for follow-up.

18. Detective Hedden is part of the Kentucky Internet Crimes Against Children (ICAC) Task Force. As part of his official duties, he conducts online enticement of children investigations, by being online portraying to be a 14-year-old girl who lives in Kentucky on the website/application Omegle.

19. In summary, on August 9, 2021, Detective Hedden, while portraying to be a 14-year-old girl (Undercover-UC), began communicating with an unknown subject (UNSUB) on Omegle. It is believed the UNSUB is 56-year-old Gregory Ortlip who lives at 1161 The Crossings Drive in O’Fallon, within St. Charles County, Missouri. The UNSUB brought up the topic of sex after the UC indicated they were 14 years old. The UNSUB requested the UC to manufacture or produce images which would be child pornography since they would have shown sexual contact by having the UC touch and expose her vagina for the purpose of gratifying the sexual desire of UNSUB. These actions are in violation of Missouri and Kentucky state law along with 18 U.S. Code §§ 2251 (sexual exploitation of children), 2252A (certain activities

relating to material constituting or containing child pornography), 2422 (coercion and enticement of a minor) and/or 1470 (transfer of obscene material to a minor).

20. Detective Hedden provided the MSHP a copy of his written report, a copy of the entire Omegle chat, and a copy of the text messages he exchanged with the UNSUB as the 14-year-old UC. I reviewed all these items. Detective Hedden's report states:

21. While authorized by the Attorney General and the Commissioner of the Department of Criminal Investigation to conduct undercover investigations within the Commonwealth, I conducted such operation on August 9, 2021. An unknown subject (UNSUB) was connected to this detective on the Omegle chat website over detectives issued undercover computer. Omegle users are connected via matched interest or search terms. In this case I was matched on the UNSUB while using the term St. Louis. At the beginning of the conversation, the UNSUB was advised the undercover (UC) was a 14-year-old female in Kentucky. After being advised of such, the UNSUB made the conversation sexual in nature. He asked about the UC's sexual history and asked to receive sexual images of the minor UC persona. The following is an excerpt of the messages from that conversation on August 9, 2021:

Start of Omegle conversation:

UNSUB: Age?
UC: 14
UNSUB: Nice
UC: How old ru
UNSUB: What part of StL
UC: im in ky
UNSUB: I'm 45
UC: k
UNSUB: What brings you here today
UC: just bored as af
UNSUB: Horny?
UC: umm idk
UC: maybe

UC: lol\

UNSUB: You like sex?

A few seconds later the conversation continued:

UNSUB: Did you suck his cock?

UC: Yea

UNSUB: And swallow his cum?

He then requested sexually explicit images from the UC:

UNSUB: Will you send me pictures of your naked body?

UC: like totally nkd?

UNSUB: Yes pussy open and everything

22. The conversation continued for several more minutes on Omegle. It eventually moved over to text message. The UNSUB provided a phone number of 314.562.1309 and requested to text. The UC provided a phone number. Once on text message, the UNSUB renewed his request to “see the UC undressed.” The conversation continued in the following days via texting.

23. On Friday, August 13, 2021, Trooper Frost contacted the St. Charles County Prosecuting Attorney’s Office and requested a subpoena be issued to AT&T for subscriber information for the phone number UNSUB used; 314.562.1309.

24. On Tuesday, August 17, 2021, a subpoena was issued by the Circuit Court of St. Charles County. The subpoena was served by St. Charles County Prosecuting Attorney’s Office.

25. On Thursday, August 19, 2021, AT&T responded to the subpoena and indicated the phone number was assigned to Gregory Ortlip and the billing and user address listed were both 1161 The Crossing Drive in O’Fallon, Missouri.

26. On August 29, 2021 Omegle responded to an investigative subpoena from the St. Charles County Prosecuting Attorney’s office. Omegle provided the metadata for the chat between UC and UNSUB a cookie was established on UNSUB’s phone for Omegle with the

value “JSDY9Z4U”. Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience. Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.

27. The Omegle chat website allows for connected users to create an archive at the end of a chat if desired. The records for the connected users for the archive are also stored on the Omegle server. The Omegle server maintains the IP records for associated archives and attached users and may be retrieved based on a unique Web Address created by Omegle for each chat. The unique Web Address associated with the above-listed communications between the UC and the UNSUB (Gregory Ortliip) is: <http://logs.omegle.com/40f56a40719600f3>.

28. MSHP Trooper J.T. Frost sent a preservation letter to Omegle.com LLC on August 13, 2021, requesting that records associated with the account <http://logs.omegle.com/40f56a40719600f3> be preserved.

29. Gregory Ortliip was charged with one count of solicitation of child pornography by Complaint in the U.S. District Court for the E.D. of Missouri in cause number 4:21-MJ-03200-NCC on August 26, 2021. He was subsequently indicted for that same offense on September 8, 2021, in cause number 4:21-CR-00501-JAR/DDN. This criminal case is pending as is a correlated case in the Circuit Court for St. Louis County, Missouri.

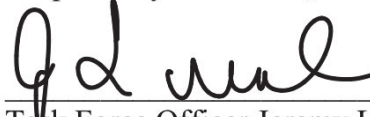
CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

I state under the penalty of perjury that the foregoing is true and correct.

Respectfully Submitted,



Task Force Officer Jeremy L. Weadon
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on 16th of December, 2021.

/s/ David D. Noce
DAVID D. NOCE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Omegle account associated with Gregory Ortlip, Cookie ID JSDY9Z4U that is stored at premises owned, maintained, controlled, or operated by Omegle.com LLC, a company headquartered at 906 West 2nd Ave, STE 100, Spokane, WA 99201.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Omegle

To the extent that the information described in Attachment A is within the possession, custody, or control of Omegle, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Omegle, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Omegle is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b) The types of service utilized by the user;
- c) All records or other information stored by an individual using the account, such as, primary records to include texts and videos, chat logs saved by user, chat

history metadata to include phone records and IP addresses used to send/receive, webcam moderation snapshots;

d) Port number and time stamp;

e) ID Cookie assigned for identification of subscriber.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) (sexual exploitation of children), 2252A (certain activities relating to material constituting or containing child pornography), 2422 (coercion and enticement of a minor) and/or 1470 (transfer of obscene material to a minor) (“target offenses”) for each account or identifier listed on Attachment A, information pertaining to the following matters:

a) Records, data, images, videos, communications, items or information relating to the commission of the target offenses;

b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

c) The identity of the person(s) who communicated with the user ID about matters relating to child pornography, including records that help reveal their whereabouts;

d) Evidence indicating the user’s state of mind as it relates to the target offenses;

- e) Evidence indicating how, when, and where the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crimes under investigation and the account subscriber, including to identify times and dates photographs and/or videos were taken;
- f) Passwords and encryption keys and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.

III. Means of Production by Omegle

Omegle shall disclose responsive data, if any, in electronic format by sending to Federal Bureau of Investigation, ATTN: TFO Jeremy L. Weadon 3065 William Street, Suite 404, Cape Girardeau, Missouri, 63701 using the United States Postal Service or another courier service

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS
PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND
902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature